Octopus Conference on Cybercrime, Strasbourg, 11 – 13 July 2018

Workshop 1: **Evidence and jurisdiction in cyberspace: multi-stakeholder consultation on the Protocol to the Budapest Convention**

Contribution by:
Christine Galvagna, German Chancellor Fellow
Global Public Policy Institute (GPPi), Berlin, Germany

Date submitted: 26 June 2018

HUMAN RIGHTS REQUIREMENTS FOR STREAMLINED ACCESS TO SUBSCRIBER DATA

In an effort to streamline cross-border access to subscriber information by law enforcement agencies, the Cybercrime Convention Committee asks whether current practices by US providers[1] can be generalized in a protocol to the Convention on Cybercrime ("Budapest Convention").[2] Specifically, this refers to the fact that US companies can disclose non-content data to foreign law enforcement agencies without a US warrant obtained through a mutual legal assistance (MLA) process.[3]

The desire to replicate this practice is an understandable response to the slow speed and inefficiency of treaty-based MLA processes, as well as the idea that subscriber information requires less stringent protection than other categories of data.[4] Direct access would allow investigators in one state to bypass the typically slow, inefficient, labor-intensive, and sometimes redundant MLA judicial proceedings in the other state.[5] Furthermore, given that subscriber information is the most commonly requested category of personal data, streamlined access would go a long way in alleviating the overall burden of MLA data requests.[6]

However, the assumption that subscriber data require far weaker legal protections – potentially none if the US system is replicated – is false. The protection of subscriber information also protects anonymous web use, which is crucial to the exercise of

---

[1] Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2702(c)(6) (Permitting a provider to disclose information to "any person other than a governmental entity") and § 2711(4) (Defining "governmental entity" as "a department of agency of the United State or any State or political subdivision thereof").
[2] Convention on Cybercrime ("Budapest Convention"), 23 Nov. 2001.
[3] ECPA §§ 2702(c)(6) and 2711(4).
[4] Cybercrime Convention Committee, T-CY Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention) (1 March 2017), p.5 ("Obtaining subscriber information may represent a lesser interference with the rights of individuals than obtaining traffic data or content data."). See also, European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (17 April 2018), p. 14 ("The intensity of the impact on fundamental rights varies . . . between subscriber data on the one hand and transactional and content data on the other hand . . . . Because of the different levels of interference with fundamental rights, it is justified to attach different conditions to subscriber data on the one hand and transactional and content data on the other, as is done in several provisions in the Regulation.").
[5] See, e.g., Fidler, MLAT Reform: Some Thoughts from Civil Society, Lawfare (11 Sept. 2015).
[6] T-CY Guidance Note #10, *supra* at n. 4, p. 3.

human rights in the digital age. Therefore, the committee must not simply strip away legal safeguards for the sake of efficiency, but rather replace them with different but equally stringent protections.

This submission highlights the human rights implications and requirements of cross-border access to subscriber data by law enforcement agencies.

What is subscriber information, and what does it reveal?

What is subscriber information?

As defined by the Cybercrime Convention, subscriber information is computer data other than traffic data and content that can establish a user's identity or address.[7] It includes basic information such as a user's name, gender, telephone number, postal or geographic address, and payment information.[8] It also includes access numbers, such as a user's IP address, telephone number, website address, domain name, or email address, as well as the type of communication service used and the period of time during which it was used.[9]

Why do investigators need it?

Subscriber information typically provides leads to investigators. Most commonly, investigators either query a person's name to determine which services or technical provisions the person uses, or they begin with an IP address or other technical address and identify the individual using it.[10]

What else does it reveal?

Indirectly, subscriber information reveals much about a user. Normally, when a user visits a website, watches or uploads a YouTube video, downloads a file, or purchases something online, a record of the interaction with the user's IP address is generated.[11] IP addresses, email addresses, and other subscriber data also generate a history of one's geographical locations.[12] This information can in turn reveal a person's associations, travel history, and much else.[13]

---

[7] Cybercrime Convention Committee, Explanatory Report to the Convention on Cybercrime (23 Nov. 2001), para. 180; Cybercrime Convention Committee, T-CY Guidance Note #8: Obtaining subscriber information for an IP address used in a specific communication within a criminal investigation (12 Nov. 2013), pp. 4–5; Budapest Convention, Article 18.

[8] Id. A target can be either an account holder or a person entitled to use the account. Explanatory Report, *supra* at n. 7, para. 177.

[9] Explanatory Report, *supra* at n. 7, para. 177.

[10] Id. para. 178. Technical provisions are "all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks)." Id. para. 179.

[11] Parsons and Israel, Canada's National Security Consultation (5 Oct. 2016).

[12] Id.

[13] Id.

Human rights implications

Because of its potential to undermine the anonymity of web use, access to subscriber information can constitute an interference with fundamental rights. Anonymity facilitates the freedoms of association, expression, opinion, and access to information, and also helps to protect privacy and personal data.[14] Therefore subscriber information must be shielded from excessive government interference by sufficiently strong legal protections in cross-border requests.

Anonymity enables the enjoyment of human rights

UN Special Rapporteur David Kaye devoted the first report of his mandate to the importance of anonymity for the exercise of the freedoms of expression and opinion:

> Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments . . . . The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression . . . . Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment."[15]

In particular, anonymity is indispensable for one's ability to develop and hold an opinion. In contrast to the right to privacy and freedom of expression, the right to hold an opinion is absolute.[16] Whereas public authorities may interfere with the right to privacy and freedom of expression when balancing them against other societal concerns, no interference with the right to hold an opinion is permitted.[17] Because we now "hold opinions digitally," in the form of web browsing histories, cloud files, and the like, restrictions on anonymity must be subject to heightened scrutiny, as they may per se violate the right to hold an opinion.[18]

---

[14] Delfi AS v. Estonia, App. 64569/09, European Court of Human Rights ("ECtHR"), Judgment, para. 147 ("Anonymity has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet."); Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/23/40, para. 23 ("Anonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation.").

[15] Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/29/32 (22 May 2015), para. 12. See also Id. paras. 16, 17, and 21; La Rue, *supra* at n. 14, paras. 47–49.

[16] International Covenant on Civil and Political Rights (ICCPR), Treaty Doc. No. 95-20 (16 Dec. 1966), Article 19(1) ("Everyone shall have the right to hold opinions without interference.").

[17] ICCPR, Article 19.

[18] Kaye, *supra* at n. 15, paras. 19–21.

Access to subscriber information undermines anonymity

In a recent case, the Supreme Court of Canada noted the relationship between subscriber information, anonymity, and the right to privacy when deeming warrantless police access to subscriber data an unconstitutional search:

> "[P]articularly important in the context of Internet usage is the understanding of privacy as anonymity. The identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information. Subscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating to an individual's identity as the source, possessor or user of that information. Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure."[19]

Similarly, the European Court of Human Rights (ECtHR) found that privacy rights were engaged by police access to subscriber information that revealed a user's identity.

> "[W]hat would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data . . . . To hold otherwise would be to deny the necessary protection to information which might reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle."[20]

It further found that warrantless police access to subscriber data violated the applicant's right to privacy. Without independent authorization, oversight, and rules governing data retention, the statutory basis lacked sufficient safeguards against abuse.[21]

Given the importance of subscriber information to anonymity, the protocol cannot simply remove all legal safeguards normally derived from MLA procedures by replicating US practices. Eliminated protections must be offset by new safeguards.

Which legal protections should apply?

Human rights legal framework

Interference with a fundamental right will violate that right if it is not accompanied by adequate legal protections aimed at preventing abuse.[22] An interference with privacy- and expression-related rights must serve a legitimate aim, be necessary to achieve that aim, proportionate to the aim, and accompanied by adequate safeguards and oversight.[23]

---

[19] R. v. Spencer, 2014 SCC 43.
[20] Benedik v. Slovenia, App. 62357/14, ECtHR, Judgment, paras. 109–10.
[21] Id. paras. 130–34.
[22] Zakharov v. Russia, App. 47143/06, ECtHR, Judgment, paras. 229–31.
[23] Kaye, *supra* at n. 15, paras. 29–35; Zakharov, paras. 227–34.

The Budapest Convention lacks such protections. It does not require parties to provide legal protections specific to the investigation of cybercrime. Instead, it reiterates parties' obligations under general-purpose human rights treaties, such as the International Covenant on Civil and Political Rights (ICCPR) and European Convention on Human Rights (ECHR), and demands that domestic law provide some sort of protection pursuant to these obligations.[24] This is problematic, because states often fail to provide adequate legal protections in relation to data collection, despite these treaty obligations.[25] Therefore the protocol must include concrete safeguards specific to the exercise of enumerated powers, including direct access to subscriber data.

Oversight

Oversight, which can take place before, during, or after data collection, is imperative. Prior judicial authorization is ideal, because it most effectively ensures independence, impartiality, and adherence to procedural safeguards.[26] Authorization by a body within the executive branch is acceptable only if it is sufficiently independent.[27] In the absence of judicial authorization, a stringent after-the-fact oversight process involving judges is necessary.[28] The involvement of technologists would also be valuable.

For example, in an older German case, the ECtHR found that authorization for surveillance by a minister was acceptable because it was complemented by sufficiently independent oversight.[29] The oversight scheme involved two bodies – one parliamentary group that included members of the opposition party, and one composed of parliamentary appointees and headed by a person qualified to be a judge.[30] These bodies reviewed the minister's orders and had the power to cancel them.[31]

Technologists should also play a key role in the oversight process. Members of parliament, bureaucrats, and judges often lack technical expertise, and consequently may not fully understand the extent and manner of personal data-related

[24] Budapest Convention, Article 15.
[25] See, e.g., Joseph Cannataci, Report of the Special Rapporteur on the right to privacy, UN Doc. A/HRC/31/64 (24 Nov. 2016).
[26] Szabó and Vissy v. Hungary, App. 37138/14, ECtHR, Judgment, para. 77 ("The Court recalls that the rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.").
[27] Id. para. 77 ("As regards the authority competent to authorise the surveillance, authorising of telephone tapping by a non-judicial authority may be compatible with the Convention, provided that that authority is sufficiently independent from the executive . . . However, the political nature of the authorisation and supervision increases the risk of abusive measures." [citations omitted]).
[28] Id. para. 77 ("The *ex ante* authorisation of such a measure is not an absolute requirement *per se*, because where there is extensive *post factum* judicial oversight, this may counterbalance the shortcomings of the authorization.").
[29] Weber and Saravia v. Germany, App. 54934/00, ECtHR, Decision, paras. 24–25 and 137.
[30] Id.
[31] Id.

interference. Governments have begun to recognize the value of technologists in oversight processes.[32]

Safeguards

Rules governing access to personal data must include the following "minimum safeguards," or conditions for access: a clear description of offenses that may give rise to an order and the categories of people whose data may be collected, a time limit for collection, procedures required for examining, using, storing, deleting and destroying data, and precautions for sharing data with other parties.[33]

These safeguards ensure that the language used to authorize data collection is not "expressed in terms of an unfettered power."[34] It would be "contrary to the rule of law" if a statute did not "indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[35]

Categories of people

Access to subscriber data should be conditioned upon individualized suspicion.[36] Without a sufficient factual basis for the suspicion of a targeted individual, a court cannot perform the required proportionality test.[37] Indiscriminate data collection or the targeting of overly broad categories of people constitutes a violation of subjects' privacy rights.[38]

The Budapest Convention's Explanatory Report states that this requirement is implied by the fact that data access takes place during a specific criminal investigation or proceeding.[39]

Nature of offenses

Offenses justifying a request for subscriber data must be clearly defined. The ECtHR has found ambiguous descriptions of offenses (e.g., "ecological security") incompatible with the ECHR.[40]

---

[32] For example, technologists have twice been nominated to the US Privacy and Civil Liberties Oversight Board. Zetter, The President's NSA Advisory Board Finally Gets a Tech Expert, Wired (17 Feb. 2016); Kerry, The White House PCLOB Nominations: A Pleasant Surprise, Lawfare (14 March 2018).
[33] Weber and Saravia, para. 95. These rules have been applied in contemporary internet surveillance cases. See, e.g., Szabó and Vissy.
[34] Weber and Saravia, para. 94.
[35] Id. (citations omitted).
[36] See, e.g., Szabó and Vissy, para. 71; Zakharov, para. 260; Tele2 Sverige AB v. PTS, C-203/15, Judgment, Court of Justice of the European Union, para. 119.
[37] Id.
[38] Zakharov, paras. 249, 263, 267. But see *Centrum för Rättvisa v. Sweden*, App. 35252/08, ECtHR, Judgment, paras. 12, 111, 112, and 124 (Implying that individualized suspicion is not necessary in foreign intelligence surveillance operations).
[39] Explanatory Report, *supra* at n. 7, para. 182 ("As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers.").
[40] Zakharov, para. 248.

Procedures for examining, using, and storing data

It is also important to set a reasonable maximum time limit for data storage, along with clearly defined conditions for renewal or exceptions.[41] If time limits are not clearly specified, retention must be subject to periodic review, so that irrelevant data are deleted.[42]

Remedy

As with any fundamental right, there must be a remedy available to individuals to challenge potential violations.[43] An individual whose data has been accessed should be notified as soon as this knowledge would not be detrimental to the investigation, so that he or she can seek a remedy if appropriate.[44] Remedies include, for example, an administrative court review of the lawfulness of the interference, a civil court action for damages, or an application to a constitutional court.[45] If access to a judicial remedy is contingent upon actual knowledge, but notification is not required, then the remedy is inadequate.[46]

Summary of required legal protections

Legal protections must include:

- Stringent oversight involving the judiciary, whether prior or subsequent to authorization
- Individualized suspicion or a similar standard that precludes indiscriminate data collection
- Clear and detailed grounds for data access and procedures for their use
- A remedy for potential abuse
- Concrete hurdles to the abuse of data access powers, rather than mere "rubber stamps"

[41] See, e.g., Weber and Saravia, para. 95 and 98–101; Benedik, para. 130. See also Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) (29 Nov. 2017), pp. 3–4.
[42] Article 29 Data Protection Working Party, supra, at pp. 3–4.
[43] ECHR, Article 13; ICCPR, Article 2.
[44] Zakharov, para. 287. Alternatively, if any individual is able to seek a remedy on the basis of mere suspicion that he or she is being surveilled, notification is not necessary. Kennedy v. United Kingdom, App. 26839/05, ECtHR, Judgment, para. 167.
[45] Klass v. Germany, App. 5029/71, ECtHR, Judgment, para 71-72.
[46] Zakharov, para. 298.

Conclusions

The Committee should recall that several parties to the Convention face serious challenges to the rule of law, such as pressure on judicial independence and abuse of law enforcement powers for political ends. Neither their legal obligations pursuant to the ICCPR or ECHR, nor their domestic laws, have fully prevented these problems. This is why the Committee should not use the protocol drafting process as an opportunity to simply shed safeguards for the sake of efficiency, and assume international obligations or existing domestic laws will fill these gaps. The protocol must compensate for the loss of existing protections by requiring states to adopt the protections outlined above.

Christine Galvagna
Global Public Policy Institute
cgalvagna@gppi.net